Enhancing e-commerce security using GSM authentication

Vorapranee Khu-smith and Chris J. Mitchell

Technical Report
RHUL–MA–2002–3
11 December 2002

Information Security Group
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

Abstract

Today, e-commerce transactions are typically protected using SSL/TLS. However, there are risks in such use of SSL/TLS, notably threats arising from the fact that information is stored in clear at the end point of the communication link and the lack of user authentication. Although SSL/TLS does offer the latter, it is optional and usually omitted since users typically do not have the necessary asymmetric key pair. In this paper, we propose a payment protocol in which user authentication is provided using GSM 'subscriber identity authentication'. In the protocol, a consumer is required to possess a GSM mobile station registered under a subscriber name corresponding to that on his/her debit/credit card. The cardholder identity is combined with the GSM subscriber identity in such a way that without a mobile station, in particular the SIM, and the corresponding debit/credit card, an unscrupulous user will find it difficult to make a fraudulent payment at the expense of the legitimate cardholder. This is achieved in such a way that no management overhead is imposed on the user.

1 Introduction

In an e-commerce transaction, a consumer typically makes a payment using a debit/credit card. The communications link between the consumer PC and the merchant server is usually protected against eavesdropping using Secure Socket Layer (SSL) or Transport Layer Security (TLS) [5]. Even so, a number of security threats remain. One reason for these remaining vulnerabilities is that SSL/TLS does not obligate client authentication. As a result, it is not easy to verify if the person who is making a payment is the legitimate cardholder. A malicious user, who may have obtained card details by some means, may then be able to use them to make payments over the Internet at the expense of the legitimate cardholder. Consequently, a way to reduce the risk of such frauds is to perform user authentication.

Apart from the lack of client authentication, using SSL/TLS to protect an e-commerce transaction poses another threat. Since SSL/TLS was designed to secure the communication link, the information is available in clear text at the destination. As a result, merchant servers have become a target for attackers who wish to obtain card numbers.

If client authentication is to be provided using public key cryptography (as supported by SSL/TLS), then the user must first establish a public key pair. He/she will also need a secure place to store the private part of the key. Usually the key is stored in the user PC and hence the user has to use

the particular machine every time a payment is to be made. Although a smart card could be employed to store the key and hence enhance mobility, not many user PCs are equipped with smart card readers. By contrast, very large numbers of users across the world now possess a GSM mobile phone.

In this paper we propose a payment protocol in which user authentication is enhanced using a GSM mobile phone (or in classic authentication model terms, something the user has). The protocol also indirectly reduces the threat posed by the storage of unencrypted card numbers in a merchant server by reducing the value of stolen card numbers to a fraudster. This is achieved by requiring the user to possess both a debit/credit card and a Mobile Station (MS), i.e. a Mobile Equipment (ME) and a Subscriber Identification Module (SIM), which must be registered under the name that appears on the card. In short, the protocol makes use of MS portability and the GSM authentication mechanism to provide user authentication in a way that also supports user mobility.

In this paper, GSM subscriber identity authentication is first described, followed by the proposed protocol. A threat analysis, and a discussion of the advantages and disadvantages of the scheme are subsequently given, followed by an overview of and comparisons with related work.

2 Subscriber identity authentication

Three main security services are provided by the GSM air interface protocol. They are subscriber identity confidentiality, subscriber identity authentication, and data confidentiality. However, subscriber identity authentication is the only security service used in the proposed protocol and hence will be the only issue described here. Details of the other security services can be found in [3, 4, 9].

In every SIM, there exists a long-term secret key, K_i, which is unique and known only to the SIM and Authentication Centre (AuC) of the home network operator of the subscriber. The home network operator is the organisation with whom the subscriber has some kind of contractual arrangement for the provision of service, and which the subscriber pays for this service.

To authenticate a SIM, the visited network needs two parameters, namely a random number ($RAND$) and a expected response ($XRES$). The ($RAND$, $XRES$) pair enables the network to verify the authenticity of the SIM without having the K_i. To compute the ($RAND$, $XRES$) pair, the AuC generates a $RAND$ and passes it with K_i as parameters to algorithm $A3$ which is specific to a network operator. The output of $A3$ is $XRES$.

$$(RAND, K_i) \xrightarrow{A3} XRES$$

The AuC generates the (*RAND*, *XRES*) pair as required, and passes them to whichever network needs them. When a SIM is requested to authenticate itself to a network, a *RAND* is sent from the network to the SIM. Since the SIM is equipped with the function $A3$ and the secret key K_i, it can generate the Signed Response (*SRES*) using *RAND* and K_i as inputs. The SIM then sends the *SRES* to the network where it is compared with the *XRES*. If they match, SIM verification is successful.

3 Using GSM authentication for electronic transactions

In this section, an e-commerce user authentication protocol which makes use of the GSM authentication service is described. In the proposed scheme, a consumer is required to have a GSM Mobile Equipment and a SIM registered under the name that appears on the debit/credit card. It is important to note that the protocol does not need the SIM to be modified in any way. However, the ME does need to have the means to take a *RAND* value from a PC, pass it to the SIM, and pass the *SRES* value from the SIM back to the PC.

In this section, the system components required are first described, followed by the transaction processing procedure.

3.1 System components

Three main system components are involved in our payment protocol. These are a User System, a merchant server, and an AuC.

3.1.1 User System

The User System consists of an MS and a PC. The MS (in fact the SIM) is responsible for outputing the *SRES*. Therefore, although an ME is needed to interact with the SIM, the protocol can work without an ME if there is an alternative means for the SIM to communicate with the user PC. The means of communication used between the MS and the user PC is not specified in this paper. However, Infrared, a cable, or Bluetooth[1] could be employed for

[1] http://www.bluetooth.com

the purpose (such means of communication are becoming commonplace as mobile devices are increasingly being used for data transfer). An alternative is to use USIM Toolkit commands [1] which enables the SIM to request the ME to open an infrared or bluetooth channel with another terminal (in this case, the user PC). However, it is worth noting that such use of USIM Toolkit requires both the SIM and the ME to support USIM Toolkit commands.

In the remainder of this paper the scheme is described in the context of a User System in which the PC provides the main platform for conducting user e-commerce, and the MS simply acts to support user authentication. However, in environments where the MS has sophisticated user interfaces and processing capabilities, e.g. a WAP or 3G phone, the MS could take on some or all of the PC's tasks.

3.1.2 Merchant server and Authentication Centre

The merchant server is the component that interacts with the User System to support electronic transactions. The merchant server also interacts with the AuC in order to retrieve values required in the user authentication process.

The Authentication Centre (AuC) is required to supply the merchant server with values necessary for the GSM identity authentication process. It takes inputs from the merchant server and produces the values used for identity authentication. The choice of the communication link between the two is again not an issue here. However, it could be the Internet or a special-purpose link provided by the mobile network operator.

As discussed in Section 4.2, we suppose that the integrity and confidentiality of the merchant server/AuC link is protected in some way, e.g. via encryption and MACs or signatures; however, the means by which this is achieved is outside the scope of the discussion here.

3.2 Transaction processing

The proposed payment protocol starts after a consumer has decided to make a payment. The decision about which purchase to make is outside the scope of this paper — we simply assume that the consumer and the merchant wish to perform a specified transaction.

The consumer first fills in a typical Internet purchase form using the PC. In this protocol however, the form is required to contain a field for a mobile phone number. Upon receipt of the form, the merchant server extracts the mobile number from the form and the identity authentication process begins. The procedure is illustrated in Figure 1.

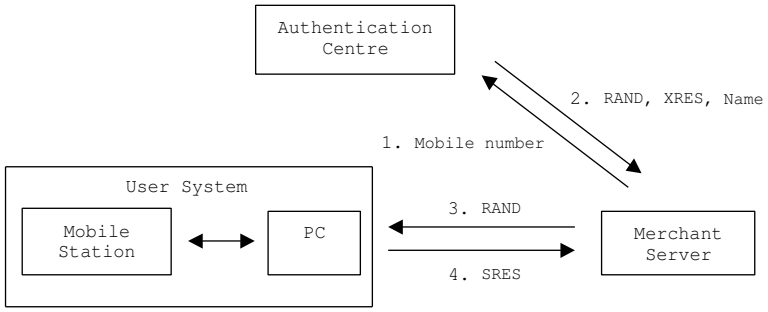

Figure 1: GSM-e-commerce identity authentication process.

The merchant server first sends the consumer's mobile number to the AuC in order to retrieve three values: a random number (*RAND*), an expected response (*XRES*), and the subscriber name. This corresponds to message 1 in the figure.

Upon receipt of the merchant server request, the AuC generates the (*RAND*, *XRES*) pair using the key K_i of the requested mobile number and algorithm $A3$. It then sends the (*RAND*, *XRES*) pair along with the name of the subscriber to the merchant server as shown in message 2 in the figure. Upon receipt of message 2, the merchant server first compares the name of the cardholder with the subscriber name received from the AuC. If they match, the *RAND* will be sent to the PC as in message 3 of the figure. Otherwise, the identity authentication process fails and the protocol ends.

After having received the *RAND*, the user PC forwards it to the ME. The ME then sends the *RAND* value to the SIM, just as it would if the *RAND* was sent via the radio interface by a GSM base station. The SIM now generates an *SRES* using the received *RAND* and its stored K_i as inputs to algorithm $A3$. The SIM then passes the generated *SRES* back to the ME, again just as it would normally (i.e. the SIM is not required to have any special functionality). The ME then sends the *SRES* to the PC which again forwards the value to the merchant server (message 4). At the merchant server, the *SRES* is compared with the *XRES*. If they match, the consumer is deemed to have been authenticated. The Internet transaction processing may now continue.

4 Threat analysis

In this section, we consider threats to the proposed protocol. The threats can be divided into three categories: threats to the User System, threats to the two communications links (user system/merchant server and merchant server/AuC), and threats in the merchant server and the AuC.

4.1 Threats in the User System

As stated previously, the User System consists of a user PC and an MS. Since the user PC does not contain sensitive information, the threats arising from the PC are minimal. Although information that passes via the PC can be cached, this information is not confidential. A debit/credit card number can be cached and compromised but the protocol still requires a corresponding SIM to make an electronic transaction.

Threats to the MS are divided into two scenarios depending on the amount of information an attacker has. Clearly, if he/she has neither the SIM nor the card details, a transaction cannot be made and hence there is no threat. It should also be clear that if the attacker has both a complete set of card details and a stolen SIM for the cardholder, then the system cannot prevent an attack — unless, of course, the SIM has been reported stolen and blacklisted by the network. We therefore consider the two main 'intermediate' scenarios.

- Scenario 1: Attacker has a stolen SIM without the corresponding card details

  In this scenario, if an attacker has stolen a SIM and the subscriber name of the stolen SIM is unknown, although a valid *SRES* can be generated, he/she will not be able to create a matched cardholder name necessary to pass the authentication process.

  By contrast, if the subscriber name is known to the attacker, it is possible for him/her to fabricate a complete set of cardholder details including a cardholder name corresponding to the subscriber name. However, the fraud becomes clear soon after the merchant tries to charge the card. In the most typical case for an e-commerce transaction, the merchant will try to charge the specified payment card before the goods are dispatched. Hence in such a case, the threat is small. Nevertheless, the threat can be more serious if the goods are, for example, information or music which will be delivered instantly via the Internet. However, even in this case, the threat can be avoided if, as is often the case, the

merchant server seeks payment authorisation before authorising delivery of the goods. If the card details are fabricated then the card issuer will, of course, reject the payment.

- Scenario 2: Attacker has stolen card details without the corresponding SIM

  If an attacker has only card details, without the SIM, it will not be possible to generate a valid *SRES*. This threat is therefore addressed by the scheme described above.

Thus, to be successful, an attack on the user system needs both the victim's SIM and the corresponding debit/credit card details to complete a fraudulent transaction.

4.2 Threats to the communications links

If any of the information transferred across either of the links is modified, then the protocol will fail. Hence, a theoretical denial of service attack exists, although there are many simpler ways to prevent the completion of a transaction. We now consider other threats arising to the two links.

4.2.1 Threats on the PC/merchant server link

The 'usual' confidentiality and integrity issues apply to the payment information transferred across this link. However we can assume that, as would typically be the case today, this link is protected using SSL/TLS. Indeed, the whole purpose of the scheme described here is to enhance the security provided by SSL/TLS rather than seeking to design a completely new and comprehensive security system. This is based on the belief that security for e-commerce must be introduced in ways which minimise the overheads for all parties, and in particular for the e-consumer.

Note that a possible alternative to the protocol described in this paper would be to use GSM authentication to enhance the security of the SSL/TLS initialisation process. However, if such an approach is followed, it is not clear how to achieve the desired link between the GSM subscriber name and the cardholder name — such an analysis is outside the scope of this paper.

4.2.2 Threats on the merchant server/AuC link

Threats on this link can be further divided into two types, namely integrity threats and confidentiality threats.

Integrity threats: There are a number of ways in which an attacker could manipulate this link in order to persuade the merchant server to accept an impostor. Perhaps the simplest method would involve the attacker using an arbitrary (valid) SIM and ME in combination with stolen card details (which, of course, will not match the GSM subscription name). In message 2 the AuC will provide a valid *RAND* and *XRES* for the attacker's SIM, and will return the name associated with the attacker's GSM subscription. An active attacker could change this name to the name associated with the stolen card details, and the merchant server will accept message 2. The remainder of the protocol will complete correctly, and the account for which the details were stolen will be charged for the transaction.

An alternative attack, again using stolen card details, does not require the attacker to have a valid SIM at all. The attacker supplies an arbitrary (but valid) GSM number with the stolen card details. In message 2, the AuC will send a (*RAND*, *XRES*) pair for the arbitrarily chosen GSM subscription, along with the subscriber name. The active attacker can then replace the contents of message 2 with the name for the stolen card details, along with an arbitrary (*RAND*, *XRES*) pair. The merchant server will accept message 2 because the names match, and will send the manipulated *RAND* to the attacker in message 3. The attacker simply returns the manipulated *XRES* value in message 4, and again the attack will succeed. The existence of these attacks means that it is vital that the integrity of the link between AuC and merchant server is protected.

Confidentiality threats: There are also a number of serious confidentiality threats. First note that a passive eavesdropper can perform an attack similar to the second integrity attack described above. Suppose an attacker has a set of stolen card details and also knows the GSM number for the owner of the stolen card details. The attacker initiates the protocol using the stolen card details and the known GSM number. Message 2 will be accepted by the Merchant server because the GSM number belongs to the valid cardholder. However, if the attacker can intercept message 2, then the *XRES* value can be obtained. The attacker then simply inserts this value into message 4 and the protocol will complete successfully.

Also note that, in the absence of integrity and confidentiality, the merchant server/AuC protocol could also be used to find the subscriber name corresponding to any GSM number. This would be a significant breach of GSM subscriber confidentiality.

These attacks mean that it is also important to provide confidentiality for this link, and this is why we assume throughout the paper that this link is both confidentiality and integrity protected.

4.3 Threats in the merchant server and the AuC

Since the merchant server is responsible for the identity authentication process, in particular the comparison of the names and *XRES* with *SRES*, it is important to protect the server against any attack which might cause the protocol to be bypassed.

Over and above the integrity of the user authentication process, the merchant server will have access to large volumes of potentially sensitive subscriber information. As part of the user authentication process, the merchant server retrieves from the AuC the account holder name for any GSM telephone number. Not only is this a sensitive privacy issue, but requiring the AuC to supply such information may potentially be in breach of its license and/or data privacy legislation. It is therefore vital that the merchant server be protected so that this information cannot be abused.

One way of mitigating this security issue is to make a slight modification to the protocol of Section 3.2. In the revised protocol, shown in Figure 2, in message 1 the merchant server supplies the cardholder name as well as the mobile number. The AuC is then required to perform the matching between the name supplied in message 1 with the name it has associated with the GSM number. If they do not match the protocol should not proceed. If they do match, in message 2 the AuC simply provides a (*RAND*, *XRES*) pair.

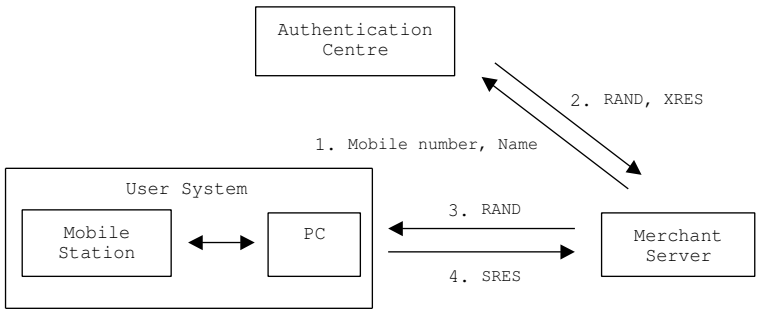

Figure 2: Revised protocol.

This modified protocol has the advantage that the AuC retains control of sensitive subscriber information. However, it has the disadvantage of requiring additional processing by the AuC.

If the integrity of the AuC could be compromised, then there are possible attacks to the security of the user authentication process. However, in such an event there are also many other serious attacks to the security of the GSM network itself, and so we assume that the AuC is well-protected.

5 Advantages and disadvantages

In this section, the advantages and disadvantages of the proposed protocol are considered.

5.1 Advantages

The following advantages arise from use of the proposed GSM-based user authentication.

1. The protocol provides user authentication based on GSM subscriber authentication. As a result, stolen credit card details cannot be used to launch a successful e-commerce transaction.

2. Since stolen credit card details cannot be used to launch a successful e-commerce transaction, the threat arising from the storage of unencrypted credit card numbers in merchant servers is accordingly reduced.

3. The protocol supports user mobility. The user authentication process requires only the correct software to be loaded on the PC, and for there to exist a means to connect the MS to the PC. In the authentication process, the PC is simply responsible for forwarding messages between the MS and the merchant server. Moreover, since the protocol does not involve storing any secrets on the PC, the risks in using untrusted PCs are minimised.

4. From the merchant point of view, the protocol will lessen fraudulent transactions and hence reduce the cost of 'card not present' chargebacks.

5.2 Disadvantages

The following disadvantages arise from use of the proposed GSM-based user authentication.

1. Prior agreement is required between the merchant and the mobile phone service provider to support the protocol between AuC and merchant server.

2. Merchants may be charged for the AuC services. This cost therefore has to be weighed against the cost of 'card not present' chargebacks which may vary from merchant to merchant. Of course, this is not a disadvantage for the GSM network provider, who may find this a useful additional revenue stream.

3. If the U-SIM Toolkit is to be used, the proposed protocol may require an ME and a SIM that support the functionality.

6 Related work

There exist other GSM-based payment systems which we now briefly review.

- The payment scheme proposed by Claessens et al. [2] provides user authentication using GSM. However, unlike the scheme discussed above, it makes extensive use of SMS messaging.

- The GiSMo (G i(nternet) S M o(pen)) scheme was developed by Millicom International Cellular in 1999. In this scheme, consumers must first open an electronic wallet over the Internet and supply their mobile phone number. Every Internet transaction is then validated with a password sent over the mobile phone using an SMS message. The GiSMo project, however, ended in 2001.

- Mint[2] and Paybox[3] are both GSM-based payment systems. They too require consumers to first open an e-wallet. Transactions in the two protocols involve either making or receiving calls using the delegated mobile phone.

- The 3-D Secure Protocol has been developed by Visa [6, 8]. The protocol aims to provide cardholder authentication for merchants using a central server called the Access Control Service (ACS). The cardholder must enroll before using the service. When a transaction is to be made, he/she will be required to enter a Personal Account Number (PAN) in addition to other information used in a traditional purchase form. The merchant then requests cardholder authentication from the ACS. The cardholder is now required to enter a password or PIN to authenticate him/herself to the ACS. The protocol can be extended to be used in mobile Internet devices such as a WAP phone [7] and the transaction flow remains similar to the one specified in [6].

Broadly speaking, the other proposed GSM-based payment systems either use SMS messaging, require e-consumers to open an e-wallet, or require them to make or receive phone calls using a GSM phone. The protocol proposed here, however, does not use any such measures. It simply utilises the GSM

[2]http://www.mint.nu

[3]http://www.paybox.co.uk

subscriber identity authentication process. The Visa 3-D Secure Protocol is similar to the proposed protocol in the way that they both aim to provide cardholder authentication. However, the Visa protocol is a complete payment security system, and is therefore much more complex than the scheme proposed here.

7 Conclusions

Today most e-commerce transactions are protected in a rather ad hoc way using SSL/TLS — this gives rise to threats, notably because of the lack of user authentication.

In this paper, we have proposed the use of GSM identity authentication to enhance e-commerce security. The protocol provides user authentication and hence significantly reduces threats arising from misuse of misappropriated card details. It therefore also indirectly reduces the risk of storing card details in unencrypted form in merchant servers. The protocol works with a 'standard' GSM SIM and requires only an appropriate equipped Mobile Equipment and a user PC. It therefore imposes minimal overheads on the user, thus increasing the likelihood of successful use. The gains for the merchant in terms of reduced chargebacks also appear significant, and the possibility of an increased revenue stream may also make the system attractive to the GSM operators.

References

[1] 3GPP. *Technical Specification Group Terminals; USIM Applicaiton Toolkit (USAT) version 5.1.0*. Third Generation Partnership Project, June 2002.

[2] J. Claessens, B. Preneel, and J. Vandewalle. Combining World Wide Web and wireless security. In B. De Decker, F. Piessens, J. Smits, and E. Van Herreweghen, editors, *Advances in Network and Distributed Systems Security*, Proceedings of IFIP TC11 WG11.4 First Annual Working Conference on Network Security, pages 153–171, Boston, 2001. Kluwer Academic Publishers.

[3] ETSI. *Digital cellular telecommunications system (Phase 2+); Security aspects (GSM 02.09 version 8.0.1)*. European Telecommunications Standards Institution (ETSI), June 2001.

[4] ETSI. *Digital cellular telecommunications system (Phase 2+); Security related network functions (GSM 03.20 version 8.1.0)*. European Telecommunications Standards Institution (ETSI), July 2001.

[5] E. Rescorla. *SSL and TLS*. Addison Wesley, Reading Massachusetts, 2001.

[6] Visa. *3-D Secure Protocol Specification: core functions version 1.0.1*. Visa International Service Association, November 2001.

[7] Visa. *3-D Secure Protocol Specification: extension for mobile Internet devices version 1.0.1*. Visa International Service Association, November 2001.

[8] Visa. *3-D Secure Protocol Specification: system overview version 1.0.3*. Visa International Service Association, December 2001.

[9] M. Walker and T. Wright. Security. In F. Hillebrand, editor, *GSM and UMTS: The Creation of Global Mobile Communication*, pages 385–406. John Wiley & Sons Ltd., 2002.